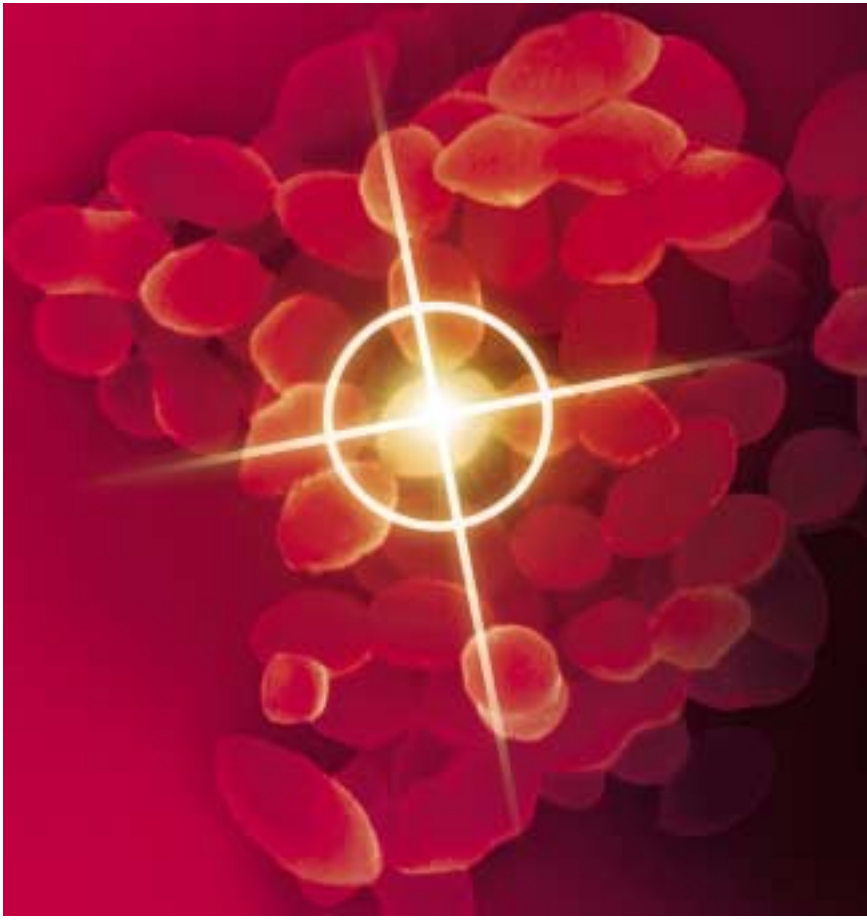
McAfee VirusScan

VERSION 6.0



McAFEE

A Network Associates Business

COPYRIGHT

© 2001, 2002 Networks Associates Technology, Inc and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

TRADEMARK ATTRIBUTIONS

ACTIVE SECURITY, ACTIVE SECURITY (IN KATAKANA), ACTIVEHELP, ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, BOMB SHELTER, CERTIFIED NETWORK EXPERT, CLEAN-UP, CLEANUP WIZARD, CNX, CNX CERTIFICATION CERTIFIED NETWORK EXPERT AND DESIGN, CYBERCOP, CYBERCOP (IN KATAKANA), CYBERMEDIA, CYBERMEDIA UNINSTALLER, DESIGN (STYLIZED N), DISK MINDER, DISTRIBUTED SNIFFER SYSTEM, DISTRIBUTED SNIFFER SYSTEM (IN KATAKANA), DR SOLOMON'S, DR SOLOMON'S LABEL, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (IN KATAKANA), EZ SETUP, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (IN KATAKANA), GUARD DOG, HELPDESK, HOMEGUARD, HUNTER, ISDN TEL/SCOPE, LANGURU, LANGURU (IN KATAKANA), M AND DESIGN, MAGIC SOLUTIONS, MAGIC SOLUTIONS (IN KATAKANA), MAGIC UNIVERSITY, MAGICSPY, MAGICTREE, MCAFEE, MCAFEE (IN KATAKANA), MCAFEE AND DESIGN, MULTIMEDIA CLOAKING, NET TOOLS, NET TOOLS (IN KATAKANA), NETCRYPTO, NETOCTUPUS, NETSCAN, NETSHIELD, NETSTALKER, NETWORK ASSOCIATES, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PC MEDIC 97, PCNOTARY, PGP, PGP (PRETTY GOOD PRIVACY), PRETTY GOOD PRIVACY, PRIMESUPPORT, RECOVERKEY, RECOVERKEY - INTERNATIONAL, REGISTRY WIZARD, REPORTMAGIC, RINGFENCE, ROUTER PM, SALESMAGIC, SECURECAST, SERVICE LEVEL MANAGER, SERVICEMAGIC, SMARTDESK, SNIFFER, SNIFFER (IN HANGUL), SNIFFMASTER, SNIFFMASTER (IN HANGUL), SNIFFMASTER (IN KATAKANA), SNIFFNET, STALKER, SUPPORTMAGIC, TIS, TMEG, TNV, TVD, TNS, TOTAL NETWORK SECURITY, TOTAL NETWORK VISIBILITY, TOTAL NETWORK VISIBILITY (IN KATAKANA), TOTAL SERVICE DESK, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, WEBSCAN, WEBSHIELD, WEBSHIELD (IN KATAKANA), WEBSNIFFER, WEBSTALKER, WEBWALL, WHO'S WATCHING YOUR NETWORK, WINGAUGE, YOUR E-BUSINESS DEFENDER, ZAC 2000, ZIP MANAGER **are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. © 2002 Networks Associates Technology, Inc. All Rights Reserved.**

McAfee Perpetual End User License Agreement – United States of America

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

    a. **Use**. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all of the Software's proprietary notices unaltered and unobstructed.

    b. **Server-Mode Use**. You may use the Software on a Client Device as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to, accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the Documentation's proprietary notices unaltered and unobstructed.

    c. **Volume License Use**. If the Software is licensed with volume license terms specified in the applicable product invoicing or product packaging for the Software, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Documentation's proprietary notices unaltered and unobstructed.

2. **Term.** This Agreement is effective for an unlimited duration unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must cease use of the Software and destroy all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable product invoicing or product packaging for the Software, you are entitled to download revisions or updates to the Software when and as McAfee publishes them via its electronic bulletin board system, website or through other online services. For a period of ninety (90) days from the date of the of original purchase of the Software, you are entitled to download one (1) revision or upgrade to the Software when and as McAfee publishes it via its electronic bulletin board system, website or through other online services. After the specified time period, you have no further rights to receive any revisions or upgrades without purchase of a new license to the Software.

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not sell, lease, license, rent, loan or otherwise transfer, with or without consideration, the Software. McAfee updates its Software frequently and performance data for its Software change. Before conducting benchmark tests regarding this Software, contact McAfee to verify that You possess the correct Software for the test and the then current version and edition of the Software. You agree not to permit any third party (other than third parties under contract with You which contains nondisclosure obligations no less restrictive than those set forth herein) to use the Licensed Program in any form and shall use all reasonable efforts to ensure that no improper or unauthorized use of the Licensed Program is made. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the applicable list price or product packaging for the Software. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by McAfee.

6. Warranty and Disclaimer.

   a. **Limited Warranty**. McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies**. McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

c. **Warranty Disclaimer**. Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MCAFEE DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL MCAFEE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE MCAFEE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF MCAFEE SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** You are advised that the Software is subject to the U.S. Export Administration Regulations. You shall not export, import or transfer Software contrary to U.S. or other applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. You represent and agrees that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Additionally, you acknowledge that the Software is subject to export control regulations in the European Union and you hereby declare and agree that the Software will not be used for any other purpose than civil (non-military) purposes. The parties agree to cooperate with each other with respect to any application for any required licenses and approvals, however, you acknowledge it is your ultimate responsibility to comply with any and all export and import laws and that McAfee has no further responsibility after the initial sale to you within the original country of sale.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). McAfee expressly disclaims any express or implied warranty of fitness for High Risk Activities.

11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. McAfee reserves the right to periodically audit you to ensure that you are not using any Software in violation of this Agreement. During your standard business hours and upon prior written notice, McAfee may visit you and you will make available to McAfee or its representatives any records pertaining to the Software to McAfee. The cost of any requested audit will be solely borne by McAfee, unless such audit discloses an underpayment or amount due to McAfee in excess of five percent (5%) of the initial license fee for the Software or you are using the Software in an unauthorized manor, in which case you shall pay the cost of the audit. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

12. **MCAFEE CUSTOMER CONTACT.** If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 988-3832, fax (408) 970-9727, or write: Network Associates, Inc., McAfee Software Division, 3965 Freedom Circle, Santa Clara, California 95054. http://www.nai.com.

McAfee Perpetual End User License Agreement – Canada

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES INTERNATIONAL B.V. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually which you acknowledge you have received and read.

    a. **Use**. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all of the Software's proprietary notices unaltered and unobstructed.

    b. **Server-Mode Use**. You may use the Software on a Client Device as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software which you acknowledge you have received and read. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to, accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the Documentation's proprietary notices unaltered and unobstructed.

    c. **Volume License Use**. If the Software is licensed with volume license terms specified in the applicable price list or product packaging for the Software, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume license authorizes. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Documentation's proprietary notices unaltered and unobstructed.

2. **Term.** This Agreement is effective for an unlimited duration unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must cease use of the Software and destroy all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable price list or product packaging for the Software, you are entitled to download revisions or updates to the Software when and as McAfee publishes them via its electronic bulletin board system, website or through other online services. For a period of ninety (90) days from the date of the of original purchase of the Software, you are entitled to download one (1) revision or upgrade to the Software when and as McAfee publishes it via its electronic bulletin board system, website or through other online services. After the specified time period, you have no further rights to receive any revisions or upgrades without purchase of a new license to the Software.

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not sell, lease, license, rent, loan or otherwise transfer, with or without consideration, the Software. McAfee updates its Software frequently and performance data for its Software change. Before conducting benchmark tests regarding this Software, contact McAfee to verify that You possess the correct Software for the test and the then current version and edition of the Software. Benchmark tests of former, outdated or inappropriate versions or editions of the Software may yield results that are not reflective of the performance of the current version or edition of the Software. You agree not to permit any third party (other than third parties under contract with you which contract contains nondisclosure obligations no less restrictive than those set forth herein) to use the Software in any form and shall use all reasonable efforts to ensure that there is no improper or unauthorized use of the Software. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the applicable list price or product packaging for the Software. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be supplied by McAfee on request and on payment of such reasonable costs and expenses of McAfee in supplying that information. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation except as expressly permitted in Section 1 above. You may not remove or alter any proprietary notices or labels on the Software or Documentation. All rights not expressly set forth hereunder are reserved by McAfee.

6. Warranty and Disclaimer.

a. **Limited Warranty**. McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

b. **Customer Remedies**. McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

c. **Warranty Disclaimer**. Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MCAFEE DISCLAIMS ALL WARRANTIES, REPRESENATIONS AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY, REPRESENTATION OR CONDITION THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL MCAFEE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE MCAFEE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF MCAFEE SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** You have been advised that the Software is subject to the U.S. Export Administration Regulations and applicable local export control laws. You shall not export, import or transfer Products contrary to U.S. or other applicable local laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. If applicable to you, you represent and agree that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government and any other applicable local authority by regulation or specific license. Additionally, you acknowledge that the Software is subject to export control regulations in the European Union and you hereby declare and agree that the Software will not be used for any other purpose than civil (non-military) purposes. The parties agree to cooperate with each other with respect to any application for any required licenses and approvals, however, you acknowledge it is your ultimate responsibility to comply with any and all export and import laws and that McAfee has no further responsibility after the initial sale to you within the original country of sale.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). McAfee expressly disclaims any express or implied warranty or condition of fitness for High Risk Activities.

11. **Miscellaneous.** This Agreement is governed by the laws of the Netherlands. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Disputes with respect to this Agreement, as well as with respect to its conclusion and execution, will be submitted exclusively to the competent court in Amsterdam. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. McAfee reserves the right to periodically audit you to ensure that you are not using any Software in violation of this Agreement. During your standard business hours and upon prior written notice, McAfee may visit you and you will make available to McAfee or its representatives any records pertaining to the Software to McAfee. The cost of any requested audit will be solely borne by McAfee, unless such audit discloses an underpayment or amount due to McAfee in excess of five percent (5%) of the initial license fee for the Software or you are using the Software in an unauthorized manor, in which case you shall pay the cost of the audit. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties have required that this Agreement and all documents relating thereto be drawn up in English. Les parties ont demandé que cette convention ainsi que tous les documents que s'y attachent soient rédigés en anglais.

12. **MCAFEE CUSTOMER CONTACT.** If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call +31 20 586 61 00 or write: McAfee, Gatwickstraat 25, 1043 GL Amsterdam, Netherlands. You will find our Internet web-site at http://www.nai.com.

Table of Contents

Chapter 1. Welcome to McAfee VirusScan 15

How Does VirusScan Software Work? 15

What Comes With VirusScan Software? 15

Chapter 2. Installing VirusScan Software 19

Before You Begin 19

System Requirements 19

Other Recommendations 20

Installation Options 21

Installation Steps 21

Troubleshooting Installation Problems 22

Important Information Regarding Windows XP Migration 24

Chapter 3. Using McAfee VirusScan 25

The VirusScan Inductive User Interface 25

Pick a Task 26

Quick Jump 27

See Also 27

About VShield Scanner 27

VShield Scanning Properties 28

How to Start and Stop VShield Scanner 29

What Should You Do When a Virus Is Detected? 29

Using Hostile Activity Watch Kernel (HAWK) 30

Using Quarantine 31

Using VirusScan With a Wireless Device 32

Data Synchronization 33

VirusScan for Palm OS 34

VirusScan for Windows CE and Pocket PC 37

VirusScan for Symbian's EPOC 39

Using Safe & Sound 40

How Safe & Sound Creates Automatic Backups 40

Defining Your Backup Strategy 41

Safe & Sound Configuration 41
Emergency Disk Creation 42

Chapter 4. Removing Infections 43
Overview 43
Removing Infections Detected Upon Installation 43
Removing an Infection In Windows 46

Chapter 5. Using McAfee Firewall 47
Overview 47
What Comes With McAfee Firewall Software? 47
How McAfee Firewall Works 48
About McAfee Firewall Documentation 49
McAfee Firewall On-line Help 49
Frequently Asked Questions 50
McAfee Firewall Configuration Assistant 52
Introduction to Firewall's new interface 54
McAfee Firewall Configurations 57
Program configuration 57
Custom settings 58
System configuration 61
Configuration After Adding/Removing Network Devices 62
Introduction to Intrusion Detection System – (IDS) 63
How to Configure the Intrusion Detection System 64

Chapter 6. Update Your McAfee Product 65
Instant Updater 65
Why Do You Need to Update? 65
How Does the Updating Process Work? 65
Instant Updater Features 65
Configuration 66

Appendix A. Product Support 67
How to Contact McAfee 67
Customer Service 67
www.McAfee-at-Home.com 68

Technical Support 68
Virus Definition Renewal 68

Index 69

Welcome to McAfee VirusScan 1

How Does VirusScan Software Work?

VirusScan software combines the anti-virus industry's most capable scan engine with top-notch interface enhancements that give you complete access to that engine's power. The VirusScan graphical user interface unifies its specialized program components, but without sacrificing the flexibility you need to fit the software into your computing environment. The scan engine, meanwhile, combines the best features of technologies that McAfee and McAfee VirusScan researchers developed independently for more than a decade.

What Comes With VirusScan Software?

VirusScan software consists of several components that combine one or more related programs, each of which play a part in defending your computer against viruses and other malicious software. These components are:

- **The VirusScan main window.** This is your central entry point in using all of the available components of McAfee VirusScan. The main window provides relevant information such as the last time a virus scan was performed on your computer and your computer's current VShield settings. The main window also informs you of the availability of updates to your product.

  Through this user-friendly interface, you access the main functions of McAfee VirusScan – simply select "Pick a task" to access and use all VirusScan features and components.

  For answers to questions about viruses, product support, or to view on-line help, refer to the See Also section of the VirusScan main window.

- **On-Demand Scanning (ODS).** On-demand scanning enables you to scan at any time. For example, if you suspect you have come in contact with an infected file, but have not accessed the file, you may manually scan the suspect file, folder, drive, etc.

- **The VShield Scanner**. This is an **On-Access Scanning** (**OAS**) component that gives you continuous anti-virus protection from viruses that arrive on floppy disks, from your network, or from various sources on the Internet. The VShield scanner starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages lets you tell the scanner which parts of your system to examine, what to look for, which parts to leave alone, and how to respond to any infected files it finds. In addition, the scanner can alert you when it finds a virus, and can summarize each of its actions.

  The VShield Scanner comes with specialized modules that guard against hostile Java applets and ActiveX controls, that scan e-mail messages and attachments that you receive from the Internet via Microsoft Mail or other mail clients that comply with Microsoft's Messaging Application Programming Interface (MAPI) standard, and that block access to dangerous Internet sites. Secure password protection for your configuration options prevents others from making unauthorized changes. The same convenient dialog box controls configuration options for all VShield modules.

- **Hostile Activity Watch Kernel.** HAWK monitors your computer for suspicious activity that may indicate a virus is present on your system. As opposed to VirusScan, which cleans the virus, HAWK prevents viruses, worms, and trojans from spreading further.

- **Safe & Sound**. This component allows you to create backup sets in protected volume files, which is the safest and preferred type of backup. A *protected volume file* is a sectioned-off area of the drive, sometimes called a logical drive.

- **Quarantine**. This component allows you to move infected files to a quarantine folder. This moves infected files from areas where they can be accessed and enables you to clean or delete them at your convenience.

- **The SendVirus utility**. This feature gives you an easy and painless way to submit files that you believe are infected directly to McAfee anti-virus researchers. A simple wizard guides you as you choose files to submit, include contact details and, if you prefer, strip out any personal or confidential data from document files.

- **The E-Mail Scan extension.** This component allows you to scan your Microsoft Exchange or Outlook mailbox, or public folders to which you have access, directly on the server. This invaluable "x-ray" peek into your mailbox means that VirusScan software can find potential infections before they make their way to your desktop, which can stop a Melissa-like virus in its tracks.

- **The Emergency Disk creation utility.** This essential utility helps you to create a floppy disk that you can use to boot your computer into a virus-free environment, then scan essential system areas to remove any viruses that could load at startup.
- **Bootable CD.** The VirusScan Installation CD includes a CD version of the emergency startup disk. If your computer is configured to start using its CD drive, then you can use the CD to boot your computer in to a virus-free environment then scan for viruses that load during startup.
- **Instant Updater.** Enables your computer to automatically communicate with McAfee while you are connected to the internet and inquire of the availability of product updates, updates to anti-virus signature files, and updates to the VirusScan scan engine. You will also use this feature to register your McAfee product.
- **Wireless device protection.** In addition to total anti-virus protection for your PC, VirusScan protects your wireless device and PC from harmful viruses transferred during the synchronization process.
- **Command-line Scanners.** This component consists of a set of full-featured scanners you can use to run targeted scan operations from the MS-DOS Prompt or Command Prompt windows, or from protected MS-DOS mode. The set includes:
  - SCAN.EXE, a scanner for 32-bit environments only. This is the primary command-line interface. When you run this file, it first checks its environment to see whether it can run by itself. If your computer is running in 16-bit or protected mode, it will transfer control to one of the other scanners.
  - SCANPM.EXE, a scanner for 16-bit and 32-bit environments. This scanner provides you with a full set of scanning options for 16-bit and 32-bit protected-mode DOS environments. It also includes support for extended memory and flexible memory allocations. SCAN.EXE will transfer control to this scanner when its specialized capabilities can enable your scan operation to run more efficiently.
  - SCAN86.EXE, a scanner for 16-bit environments only. This scanner includes a limited set of capabilities geared to 16-bit environments. SCAN.EXE will transfer control to this scanner if your computer is running in 16-bit mode, but without special memory configurations.
  - BOOTSCAN.EXE, a smaller, specialized scanner for use primarily with the Emergency Disk utility. This scanner ordinarily runs from a floppy disk you create to provide you with a virus-free boot environment.

All of the command-line scanners allow you to initiate targeted scan operations from an MS-DOS Prompt or Command Prompt window, or from protected MS-DOS mode. Ordinarily, you'll use the VirusScan application's graphical user interface (GUI) to perform most scanning operations, but if you have trouble starting Windows or if the VirusScan GUI components will not run in your environment, you can use the command-line scanners as a backup.

Installing VirusScan Software 2

Before You Begin

McAfee distributes VirusScan software in two ways:

1. As an archived file that you can download from the McAfee web site.
2. On CD-ROM.

Although the method you use to transfer VirusScan files from an archive obtained via download differs from the method you use to transfer files from a CD that is placed in your CD-ROM drive, the installation steps followed after that are the same for both distribution types. Review the system requirements shown below to verify that VirusScan software will run on your system.

System Requirements

To install this product, you require the following:

Desktop and Notebook Computers

- Windows 95B, Windows 98, Windows Me, Windows NT Workstation with Service Pack 4 or later, Windows 2000 Professional, Windows XP Home Edition, or Windows XP Professional.
- Internet Explorer 4.01, Service Pack 2 or higher required for Windows 95 and Windows NT; IE 5.01 or later recommended.
- 35 megabytes (MB) of hard disk space.
- 32 MB of RAM.
- An Intel Pentium-class or compatible processor rated at 100 MHz or higher.
- CD-ROM drive.
- Internet access for product updating.

Additional Requirements for Wireless Devices

Palm OS and Palm Requirements

McAfee VirusScan for Palm Desktop with HotSync Manager 3.0 will install and run on any IBM PC or PC-compatible computer equipped with Palm Desktop 3.0 or later. The latest version of Palm Desktop and HotSync 3.0 is a free download from Palm's site (at www.palm.com). The device-resident portion is quite simple and should work on any device with the Palm OS.

Windows CE or Pocket PC System Requirements

McAfee VirusScan for Windows CE or Pocket PC will install and run on any IBM PC or PC-compatible computer equipped with ActiveSync 3.0 or later. Any CE device with ActiveSync 3 will function properly.

Symbian EPOC System Requirements

McAfee VirusScan for Symbian's EPOC will install and run on any IBM PC or PC-compatible computer equipped with PsiWin 2.3 (or equivalent for non-Psion EPOC devices. All EPOC devices should ship with PsiWin 2.3 /EPOC Connect 5. These include:

- Psion Revo
- Psion Series 5mx
- Psion Series 7
- Psion netBook
- Oregon Scientific Osaris
- Ericsson MC218
- Ericsson R380

If you have an older device but the current PsiWin/EPOC Connect software, McAfee VirusScan for Symbian's EPOC will function properly, including the Psion HC, the MC series, the Workabout series, all Psion Series 3 models, the Psion Sienna, the Psion Series 5, the Geofox One, and the Phillips Illium.

If you do not have PsiWin 2.3, Symbian offers a free product called EPOC Connect Lite which also works.

Other Recommendations

To take full advantage of VirusScan software's automatic Instant Updater features, you should have an Internet connection, either through your local-area network, or via modem and an Internet service provider.

Installation Options

The "Installation steps" section describes how to install VirusScan software with its most common options on a single computer or workstation. You can choose to do a Typical setup – which installs commonly used VirusScan components – or you can choose to do a Custom setup, which gives you the option to install all VirusScan components.

Installation Steps

After inserting the McAfee VirusScan installation CD into your computer's CD-ROM drive, an Autorun image should automatically display. To install McAfee VirusScan software immediately, click **Install McAfee VirusScan**, then skip to Step 5 to continue with Setup.

Use the steps below to install your software.

1. If your computer runs Windows NT Workstation v4.0, Windows 2000 Professional, or Windows XP, log on to your system as a user with administrative rights. You must have administrative rights to install this software on your system.
2. Insert the McAfee VirusScan CD in to your computer's CD-ROM drive. If the McAfee VirusScan Installation Wizard does not automatically display, go to Step 3. Otherwise, skip to Step 4.
3. Use the following procedure if the Autorun installation menu does not display, or, if you obtained your software via download at a McAfee web site.
   a. From the Windows Start menu, select **Run**.
   The Run dialog box displays.
   b. Type `<X>:\SETUP.EXE` in the text box provided, then click **OK**.

   Here, `<X>` represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted McAfee VirusScan files. To search for the correct files on your hard disk or CD-ROM, click **Browse**.
4. Before proceeding with the installation, Setup first checks to see whether your computer already the Microsoft Windows Installer (MSI) utility running as part of your system software.

a. If your computer runs Windows XP, Windows Me, or Windows 2000, MSI already exists on your system. If your computer runs an earlier Windows release, you may still have MSI in your computer if you previously installed other software that uses MSI. In either of these cases, Setup will display its first wizard panel immediately. Skip to Step 5 to continue.

b. If Setup does not find MSI or an earlier version of MSI is installed in your computer, it installs files necessary to continue the installation, then prompts you to restart your computer. Click **Restart System.** When your computer restarts, Setup will continue from where it left off.

5. Refer to steps displayed on the McAfee VirusScan Installation Wizard to complete your installation.

TIP: If your computer does not have the required fonts to view the End User's License Agreement (EULA), then you may locate the appropriate EULA on your McAfee software installation CD. You must read and agree to the terms of the agreement to complete your installation.

Troubleshooting Installation Problems

A failed installation can cause software problems that are difficult to track down. The major causes of installation failure are:

- Hard drive errors.
- Temporary files that conflict with the installation.
- Attempting to install while other software is running.

Follow the procedure outlined below to minimize the affect that these common conditions may have on your installation.

Step 1: Clean up your hard drive

Run the Windows 95 hard drive utilities, ScanDisk and Disk Defragmenter to identify and fix any errors on your hard drive:

1. Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click ScanDisk.
2. In the ScanDisk window, select Standard and Automatically fix errors.

NOTE: These are the default settings.

3. Click Advanced. In the Advanced Settings dialog box, make sure the following settings are selected:
   - Only if errors found
   - Replace log
   - Delete
   - Free
4. Ignore the other options, and click OK. Click Start. ScanDisk begins scanning your drive for errors. Depending on the size of your hard drive, ScanDisk may take several minutes to complete its job.
5. When ScanDisk is finished, close ScanDisk.
6. Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click Disk Defragmenter.
7. Click OK to start Disk Defragmenter. Depending on the speed of your computer and the size of your drive, this may take several minutes to complete.
8. Close Disk Defragmenter when it has finished defragmenting your disk.

Step 2: Remove temporary files

Delete the contents of the Windows Temp folder:

1. Double-click the My Computer icon on your desktop. The My Computer window opens. Double-click the C: drive. You are now viewing the contents of your hard drive.
2. Double-click the Windows folder.
3. In the Windows folder, double-click the Temp folder.
4. In the menu, click Edit, then click Select All. All of the items in your Temp folder are highlighted.
5. Press the Delete key on your keyboard to delete the files. If Windows asks about deleting files, click Yes.
6. In the Windows taskbar, click Start, then click Shut Down.
7. Click Restart the computer, then click Yes in the Shut Down Windows dialog box to restart your PC.

Step 3: Close other software

Disable all software running in the background:

1. Hold down the Ctrl and Alt keys on your keyboard, and then press the Delete key once. The Close Program dialog box appears.
2. Click End Task for every item on the list except Explorer.
3. Repeat steps 2 and 3 until you've closed everything except Explorer.
4. When you see only Explorer in the Close Program dialog box, click Cancel. You are now ready to install your new software.

Important Information Regarding Windows XP Migration

Upgrading your computer's operating system from any version of Windows to Windows XP causes all McAfee products installed before migration to become disabled after migration to Windows XP.

You will be made aware of this situation as you make you first attempt to start a McAfee product (after migration) - you will be instructed to reinstall the product.

As such, you will need to uninstall all McAfee products and reinstall using your installation CD or the software obtained from McAfee via download.

Using McAfee VirusScan 3

The VirusScan Inductive User Interface

Under the guidance of the Microsoft Corporation, McAfee introduces a new look to McAfee VirusScan - the Inductive User Interface (IUI).

What is an Inductive User Interface?

An IUI is similar to common web-style design – each screen within the application focuses on a unique, clearly stated, fundamental purpose. An IUI also allows you to easily navigate from one screen to the next.

How will an IUI help me?

IUI simplifies using McAfee VirusScan. On any screen within VirusScan, you can easily determine how to complete a task or how to access another related or different task. You can easily navigate VirusScan by selecting the **Back**, **Forward** and **Home** icons. These three icons are common to all VirusScan screens.

How do I use the IUI?

First, start VirusScan from the Windows Start menu.

Figure 3-1. The VirusScan Main Window

The VirusScan main window is your central entry point to all VirusScan tasks, features, and components. The main window displays three regions common to all VirusScan screens.

Pick a Task

Select **Pick a task** to access the primary task screen. From the primary task screen you can select one of the following tasks:

- **Scan my computer for viruses now**.
- **Change my VirusScan settings**.
- **Manage quarantined files**.
- **Create an emergency disk**.
- **View VirusScan's activity logs**.

TIP: After picking a task, simply follow the on-line instructions to complete the task. If you would like to start a new task, select **Pick a task**.

Quick Jump

The **Quick Jump** section allows you access a function or program associated with McAfee VirusScan (a function or program may include collection of tasks). For example, from the Quick Jump section you can:

- Select **Scan for Viruses Now** to have the application scan your computer for viruses with the last configuration options you set, or with default options.
- Select **Run Safe & Sound** to display the Safe & Sound window and configure your back-up file settings.
- Select **Check for VirusScan Update** to start McAfee's Instant Updater. Instant Updater allows you to download updates to your product, anti-virus signature (DAT) files, and virus scan engine.

See Also

The **See Also** section displays links to external resources to help you use McAfee VirusScan. From the See Also section you can:

- Select **Virus Information Library** to start your internet browser and go to the McAfee A.V.E.R.T. (Anti-Virus Emergency Response Team) web site. Here you will find up-to-date information about known viruses, their symptoms, and download DAT file updates.
- Select **Visit McAfee on the Web** to start your internet browser and go to www.McAfee-at-Home.com. Our McAfee-at-Home web site is a valuable resource for all of your McAfee VirusScan support needs.
- Select **Technical Support** to start your Internet browser and go to www.mcafeehelp.com Here at www.mcafeehelp.com you will find solutions to all of your technical needs

---

TIP: Click **X** in the upper right corner of any VirusScan screen to close the VirusScan main window.

About VShield Scanner

The VShield scanner has unique capabilities that make it an integral part of the VirusScan comprehensive anti-virus software security package. These capabilities include:

- **On-access scanning**: This means that the scanner looks for viruses in files that you open, copy, save, or otherwise modify, and files that you read from or write to floppy disks and network drives. It therefore can detect and stop viruses as soon as they appear on your system, including those that arrive via e-mail or as downloads from the Internet. This means you can make the VShield scanner both your first line of anti-virus defense, and your backstop protection in between each scan operation that you perform. The VShield scanner detects viruses in memory and as they attempt to execute from within infected files.
- **Automatic operation**: The VShield scanner integrates with a range of browser software and e-mail client applications. VShield Scanner starts when you start your computer, and stays in memory until you shut it or your system down.
- **Malicious object detection and blocking**: The VShield scanner can block harmful ActiveX and Java objects from gaining access to your system, before they pose a threat. The scanner does this by scanning the hundreds of objects you download as you connect to the web or to other Internet sites, and the file attachments you receive with your e-mail. It compares these items against a current list of harmful objects that it maintains, and blocks those that could cause problems.
- **Internet site filtering**: The VShield scanner comes with a list of dangerous web- or Internet sites that pose a hazard to your system, usually in the form of downloadable malicious software. You can add any other site that you want to keep your browser software from connecting to, either by listing its Internet Protocol (IP) address or its domain name.

VShield Scanning Properties

The VShield scanner consists of five related modules, each of which has a specialized function. You can configure settings for all of these modules in the VShield Properties dialog box. The VShield modules are:

- **System Scan.** This module looks for viruses on your hard disk as you work with your computer. It tracks files as your system or other computers read files from your hard disk or write files to it. It can also scan floppy disks and network drives mapped to your system.
- **E-Mail Scan.** This module scans e-mail messages and message attachments that you receive via interoffice e-mail systems, and via the Internet. It scans your Microsoft Exchange or Outlook mailbox systems. It works in conjunction with the Download Scan module to scan Internet mail that arrives via Simple Mail Transfer Protocol (SMTP) or Post Office Protocol (POP-3) sources.

- **Download Scan.** This module scans files that you download to your system from the Internet. If you have enabled the Internet mail option in the E-Mail Scan module, this will include e-mail and file attachments that arrive via SMTP or POP-3 e-mail systems, which include such e-mail client programs as Eudora Pro, Microsoft Outlook Express, Netscape mail, and America Online mail.
- **Internet Filter.** This module looks for and blocks hostile Java classes and ActiveX controls from downloading to and executing from your system as you visit Internet sites. It can also block your browser from connecting to potentially dangerous Internet sites that harbor malicious software.
- **Hostile Activity Watch Kernel.** HAWK monitors your computer for suspicious activity that may indicate a virus is present on your system. As opposed to VirusScan, which cleans the virus, HAWK prevents viruses, worms, and trojans from spreading further.

How to Start and Stop VShield Scanner

Use the steps below to start and stop VShield Scanner.

1. With the VShield Scanner running, from the Windows taskbar select Start > Settings > Control Panel.
   The Windows Control Panel displays.
2. Double–click the VirusScan icon.
   The VirusScan Services dialog box displays.
3. Select the Service tab and Click Stop.
   VShield Scanner stops.

TIP: You can start or re-start the VShield Scanner using the steps described above.

4. VShield Scanner, by default, is configured to automatically start each time your computer starts. To prevent VShield Scanner to run at startup, clear the **Load on startup** check box.

What Should You Do When a Virus Is Detected?

First of all, don't panic! Although far from harmless, some viruses that infect your personal computer or wireless device may destroy data or render it unusable.

It can interfere with the normal operation of your computer or wireless device and may also have other undesirable effects. You should take them seriously and be sure to remove them when you encounter them.

McAfee VirusScan makes it easier for you to handle viruses whenever it is detected. Through an alert message dialog box, you are given options that you can perform simply by selecting the desired course of action.

When McAfee VirusScan detects a virus, an alert message is displayed to notify you and provide options on how you would want to proceed.

The following options are available:

- Click **Clean** if you want McAfee VirusScan to clean the infected file.
- Click **Delete** if you want McAfee VirusScan to delete the file.
- Click **Continue** if you do not want McAfee VirusScan to take any action and should just continue to scan other files.
- Click **Quarantine** to isolate the infected file from the other files, programs, and drives in your computer.
- Click **Stop** to end all running processes.
- Click **More Info**... if you want additional information about the virus found.

Using Hostile Activity Watch Kernel (HAWK)

Hostile Activity Watch Kernel (HAWK) is a VirusScan option that enables constant monitoring for suspicious activity that may indicate a virus is present on your system. Suspicious activity includes:

- An attempt to forward e-mail to a large portion of your address book.
- Attempts to forward multiple e-mail messages in rapid succession.
- E-mail attachments containing program files (executable files with an .exe file extension) or scripts that can be used to mask the actual type document transmitted to you.

Although VirusScan does an excellent job detecting known viruses, it cannot detect new viruses without a DAT file update. By monitoring for these typically malicious activities, HAWK notifies you and lets you take action before damage occurs. HAWK can prevent viruses, worms, and trojans from spreading further, while VirusScan cleans the virus to remove it from your computer.

Using Quarantine

Many VirusScan components allow you to move infected files to a quarantine folder. This moves infected files from areas where they can be accessed and enables you to clean or delete them at your convenience.

Managing Quarantined Files

This list describes the options available to you when managing quarantined files:

- **Add.** Select this option to browse for and quarantine a suspected file.
- **Clean.** Select this option to remove the virus code from infected file. If the virus cannot be removed, it will notify you in its message area.
- **Restore.** Select this option to restore a file to its original location.

WARNING: This option does not clean the file. Make sure the file is not infected before selecting Restore.

- **Delete.** Select this option to delete the infected file. Make sure to note the file location so you have a record of the deleted files. You will need to restore deleted files from backup copies.
- **Submit to McAfee.** Select this option to submit new viruses to McAfee's investigative labs.

NOTE: McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses, Java classes, ActiveX controls, or dangerous web sites that VirusScan does not now detect.

If you have found what you suspect to be a new or unidentified virus, send the infected file to McAfee Labs Anti-Virus Emergency Response Team for analysis, using the Submit to McAfee Wizard. You are given the option of removing your personal data from the file before submitting it.

Network Associates reserves the right to use any information you supply as it deems appropriate without incurring any obligations whatsoever.

- **Properties.** Select this option to discover the characteristics of the quarantined file. For example, characteristics include: file type, size, origin of file (not the suspected virus), etc.

- **Refresh.** Select refresh to update the details of files displayed in the list of quarantined files.

Using VirusScan With a Wireless Device

As the demand for wireless devices continue to grow, it carries with it, the threat of compromising your data against viruses especially whenever you exchange information between your PC and your wireless device.

Wireless devices that are currently available in the market today are primarily designed as a more convenient alternative in storing and retrieving information such as personal activities, people's addresses, telephone numbers, appointments, expenses, etc. Either at work or at home, you can easily keep track of records in all of these areas by simply using your wireless device. You can even set an alarm to alert you of important meetings, events or tasks to do during the day, week or month.

McAfee VirusScan is an application designed to protect your data by scanning the files on your wireless device every time a data exchange or update is performed with your computer. It protects your system from viruses that may have been placed on your wireless device during the use of features such as infrared transfers and wireless transactions. McAfee VirusScan supports most types of wireless devices using Palm OS, Pocket PC, Windows CE, and EPOC operating systems (please refer to the following table).

Table 3-1. Examples of wireless devices that McAfee VirusScan supports

Operating system	Wireless Device	Manufacturer
Palm OS	• Palm Handheld	Palm, Inc.
	• Palm VII Series	
	• Palm V Series	
	• Palm III Series Palm M Series	
	• Visor	HandSpring
	• Visor Edge	
	• Clie	Sony
Pocket PC	• E-115	Casio

Table 3-1. Examples of wireless devices that McAfee VirusScan supports

Operating system	Wireless Device	Manufacturer
	• iPAQ	Compaq
	• iPAQ H3600 Series	
	• Aero	
	• Aero 2100 Series	
	• PPT 2700 Series	Symbol Technologies
	• Jornada 540	Hewlett-Packard
	• Jornada 680	
	• Jornada 720	
	• E125	Cassiopeia
	• EM500	
Windows CE	• PenCentra 130	Fujitso
	• HPW-600 ET	Hitachi
	• WorkPad z50	IBM
EPOC	• Psion Series 5MX	Psion PLC
	• Psion - Revo	
	• Mako	Diamond

Data Synchronization

Data synchronization is a standard feature of most wireless operating systems wherein information or records are synchronized between a wireless device and a regular PC. This feature has been commonly known, depending on the type of device you are using as: HotSync for Palm OS devices; ActiveSync for Pocket PC's and Windows CE; and Psion Synchronizer for EPOC devices.

As an example, if you add a new entry on your wireless devices' Address List, this new entry is automatically added into the PC platform after performing a data synchronization operation. To reduce the time it takes to complete the synchronization of data on both platforms, it only changes the data that has been modified, updated or added.

In performing a data exchange operation, a data synchronization manager (i.e.: HotSync Manager, ActiveSync or Psion Synchronizer) must be running. This is the application that makes the data synchronization operation possible. It monitors your computer and responds to any data synchronization-related command when initiated from the wireless device.

> **NOTE:** Depending on the operating system on your wireless device, please refer to "Additional Requirements for Wireless Devices," on page 20 to determine the type and version of data synchronization manager (i.e.: HotSync Manager, ActiveSync) you must have to be able to use McAfee VirusScan.

VirusScan analyzes the data transmitted between your computer and your wireless device during data synchronization. If VirusScan detects the presence of infected data, you can treat the infected file in the same manner as you would any other infected file. For more information about this topic, see "What Should You Do When a Virus Is Detected?," on page 29.

VirusScan for Palm OS

About Palm OS

Palm OS developed by Palm, Inc. is one of the most common types of operating systems used for wireless computing devices. It is designed specifically for mobile information management. Through a wireless device, you can readily access personal or business information synced on at any time, and importantly, in any location.

One of its important components is HotSync data conduit synchronization technology that allows you to exchange information between your wireless device and your computer.

McAfee VirusScan for Palm OS scans your device for viruses before you can download a virus to your computer. It uses a PC-side component and a device-side component to scan the device during a HotSync with the PC.

Starting Palm Anti-Virus Components

Tap the McAfee VirusScan for Palm OS icon and several option checkboxes buttons appear on your device. These options are:

- Scan at start of a HotSync.
- Scan at end of HotSync.
- Scan Applications.
- Scan Application Data.
- Modified Records Only.
- Known File Types Only.
- Known Executable Types Only.

- Scan Flash Memory.

Available Options On the Device Component

The available wireless device component options allow you to customize how you want McAfee VirusScan to work on the components of your device. Selecting the option that you need most will help optimize your protection and scanning time.

NOTE: Changing options on either the device or the PC side component of the application changes both sides on sync. The only files scanned are files that go through the conduit to and from the device.

- Scan at start of a HotSync.
  This option allows you to scan files at the beginning of the HotSync.
- Scan at end of a HotSync.
  This option scans files at the end of the HotSync.
- Scan Applications.
  This option allows you to scan your applications.
- Scan Application Data.
  This option allows you to scan your application data.
- Modified Records Only.
  This option allows you to only scan data records that have been changed since the last HotSync operation.
- Known File Types Only.
  This option allows you to only scan known database type files.
- Known Executable Code Types Only.
  This option allows you to only scan known executable type files.
- Scan Flash Memory.
  This option allows to only scan flash memory of your wireless device to detect if a virus is present.

TIP: You can select any combination of the above scanning options.

Available Options On the PC Component

> **NOTE:** McAfee VirusScan requires that the PC-side component be installed on the PC that you will sync the wireless device with for full anti-virus protection. You will not be able to scan your device for viruses if the PC-side component of McAfee VirusScan is not installed.

The available PC component options allow you to customize how you want McAfee VirusScan to work. Selecting the option that you need most will help optimize your protection and scanning time.

What to Scan Options

- Scan Applications.
  This option allows you to scan your applications transferred to your device.
- Scan Application Data.
  This option allows you to scan application data transferred to your device.
- Modified Records Only.
  This option allows you to only scan data records that have been changed since the last HotSync operation transferred to your device.
- Known File Types Only.
  This option allows you to only scan known database type files transferred to your device.
- Known Executable Code Types Only.
  This option allows you to only scan known executable type files transferred to your device.
- Scan Flash Memory.
  This option allows you scan the flash memory of your wireless device to detect if a virus is present.

> **NOTE:** You can select any combination of the above scans.

When to Scan Options

The following are other available options that can further optimize the way McAfee VirusScan will work on your wireless device.

- At the start of each HotSync.
  This option allows you to scan your wireless device for viruses at the start of each HotSync.

- At the end of each HotSync.
  This option allows you to scan your device for viruses at the end of each HotSync.

Other Options

After selecting your scan settings, you can do any of the following:

- Click OK to accept the changes to your scan and update settings.
- Click Cancel to ignore the changes and close the window.

Removing McAfee VirusScan for Palm OS Components

Use the steps below to remove McAfee VirusScan from your device-side components.

1. From the main applications screen, tap the clock.
2. From the App menu, choose Delete.
3. Select McAfee VirusScan from the menu, and then tap the Delete button.
4. Tap Yes in the Delete Application window.
5. Tap Done to close the screen.

TIP: If you accidentally delete McAfee VirusScan from your Palm device, a backup file is available in your Palm backup directory. This file is usually listed as Palm \"username"\Backup \PalmAV.PRC, though doing a search for PalmAV.PRC will also find the file. Once you locate the file, double-click it to add it to the Palm Install Tool. The next time you HotSync your device, McAfee VirusScan will be restored.

VirusScan for Windows CE and Pocket PC

NOTE: The features and functionality associated with McAfee VirusScan for Windows CE work similarly to those of Pocket PCs. This section applies to both operating systems.

About Windows CE

Microsoft's Windows CE is an operating system platform that offers a broad range of communications, entertainment and mobile-computing devices. One of its main features is its capability to share information with Windows-based computers. It is a compact and portable operating system used on a variety of communication devices such as wireless PCs, digital information pagers and cellular smart phones.

For more information on wireless products using Windows CE, visit their Web site at www.pocketpc.com.

About Pocket PC

Pocket PCs do not only organize information. In addition to being able to seamlessly link information to your computer, it also allows you to read e-mail messages and browse the Web. Manufacturers of this type of wireless device include companies like Hewlett Packard, Casio Computer Co., Ltd., and Compaq. For examples of Pocket PC wireless devices please visit www.pocketpc.com.

Available Options On the PC Component

The available PC component options allow you to customize how you want McAfee VirusScan to work with your device. Selecting the options that you need most will help optimize your protection and scanning time.

What to Scan Options

- Scan All files.
  This option allows you to scan all files on your wireless device.
- Program Files Only.
  This option allows you to only scan those files most frequently used by your wireless device.
- New or Modified Files Only.
  This option allows you to only scan data records that have been changed or been created since the last scan operation.
- Scan files marked as in-ROM.
  This option allows you to scans files presently flagged as “in-ROM.”

When to Scan Options

The following are other available options that can further optimize the way McAfee VirusScan will work on your wireless device.

- Scan when a CE device connects to this PC.
  This option allows you to scan any Windows CE or Pocket PC device that you synchronize to your computer.

Other Options

After selecting your scan settings, you can do any of the following:

- Click OK to accept the changes to your scan and update settings.
- Click Cancel to ignore the changes and close the window.
- Click Update Now to manually begin a check for anti-virus signature updates.
- Click Scan Now to start a virus scan on your wireless device.

VirusScan for Symbian's EPOC

About EPOC

Symbian is a company that develops mobile wireless operating systems. It makes use of the EPOC operating system capable of delivering applications and communications in a small package (i.e.: wireless devices). For more information, you can visit the company Web site at www.symbian.com.

Available Options On the PC Component

The available options allow you to customize how you want McAfee VirusScan to work on your wireless device. Selecting the option that you need most will help optimize your protection and scanning time.

What to Scan Options

- Scan All files.
  This option allows you to scan all files on your wireless device.
- Program Files Only.
  This option allows you to only scan those files most frequently used by your wireless device.
- New or Modified Files Only.
  This option allows you to only scan data records that have been changed or have been created since the last scan operation.

When to Scan Options

The following are other available options that can further optimize the way McAfee VirusScan will work on your wireless device.

- Scan when an EPOC device connects to this PC.
  This option allows you to scan any EPOC device you synchronize to your computer.
- Close all programs on the EPOC device before scanning.
  This option allows you to close programs before performing a virus scan.

Other Options

After selecting your scan settings, you can do any of the following:

- Click OK to accept the changes to your scan and update settings.
- Click Cancel to ignore the changes and close the window.
- Click Update Now to manually begin a check for anti-virus signature updates.
- Click Scan Now to start a virus scan on your wireless device.

❑ **NOTE:** If you want to find out the versions of the scan engine and anti-virus signature files (DAT) that McAfee VirusScan is using to detect any problem on your wireless device, click About. This dialog box also displays dates that will allow you to determine if there is a need to update your DAT files to ensure maximum virus protection on your wireless device.

Using Safe & Sound

Safe & Sound is a unique backup utility that automatically creates backup files of your documents as you work on them.

You can configure Safe & Sound to back up to a different drive, across a network connection, or to a protected area within your local (c:\) drive.

If your files become corrupted due to a virus, or your system crashes, or if you lose your files, McAfee's Safe & Sound utility provides you the ability to recover files using the Safe & Sound Windows or DOS recover utility.

How Safe & Sound Creates Automatic Backups

When you select to have Safe & Sound automatically create a backup set for you, it creates the first backup set while you are stepping through the Safe & Sound Wizard. Thereafter, while the Enable Automatic Backup option is selected, it continues to update your backup set at the time delay you've specified. If you chose to make Mirror backups, Safe & Sound updates your backup set at the same time that you re-save the original source files.

Defining Your Backup Strategy

After you decide which backup type you want to use (either a protected volume file or a directory backup set), the most important questions you must answer when defining your own backup strategy are:

Where Will You Store the Backup Set?

In today's computer marketplace, you may discover that it is as cost effective to acquire a separate backup hard drive where you can keep a current mirror backup copy of one or more other drives that you use on your PC.

In addition, you may want the backup copy to be stored at a remote location, for increased protection. As long as Safe & Sound can access a logical drive mapped on your PC, it can store the backup set there. That is, the backup set can be stored on a shared network drive.

What Files Are Important (Which Files Must Be Backed Up)?

Safe & Sound automatically selects files that are typically important to include in a backup set. However, you can select other files or types of files to include in your backup set.

How Often Should You Or Safe & Sound Make These Backups?

The more recent your backup set, the happier you'll be if your PC does encounter a problem that compromises the data on your primary drives. However, you may want to keep the default Write-behind Delay of 20 minutes to give you time to recover a previous version of a file if you ever need to

Safe & Sound Configuration

The Safe & Sound setup wizards guides you through your initial setup. Please access on-line help for information about Safe & Sound configuration.

Use the steps below to access Safe & Sound on-line help.

1. Start Safe & Sound from the Windows Start menu.
   The Safe & Sound interface displays.
2. Click Help.
   The Safe & Sound Help window displays.
3. Click Help Topics.
   The Contents tabs of the Help Topics: Safe & Sound window displays.
4. Select the desired Help topic.

5. Double-click the help topic or click display to view the contents of the Help topic.

Emergency Disk Creation

As it installs itself, VirusScan software will examine your computer's memory and your hard disk's boot sectors to verify that it can safely copy its files to your hard disk without risking their infection. During that installation, Setup offers to create an Emergency Disk you can use to start your system in a virus-free environment. Should the VirusScan software itself become infected, or if you want to be sure your computer is clean before you install any other software, create and use an Emergency Disk to start your computer.

VirusScan software comes with an Emergency Disk wizard that makes disk creation simple and fast.

The Emergency Disk you create includes BOOTSCAN.EXE, a specialized, small-footprint command-line scanner that can scan your hard disk boot sectors and Master Boot Record (MBR). BOOTSCAN.EXE works with specialized set of virus definition (.DAT) files that focus on ferreting out boot-sector viruses. If you have already installed VirusScan software with default Setup options, you'll find these.DAT files in this location on your hard disk:

C:\Program Files\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx

The special .DAT files have these names:

- EMCLEAN.DAT
- EMNAMES.DAT
- EMSCAN.DAT

McAfee periodically updates these .DAT files to detect new boot-sector viruses. You can download updated Emergency .DAT files from this location:

http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/tools.asp

---

NOTE: McAfee recommends that you download new Emergency .DAT files directly to a newly formatted floppy disk in order to reduce the risk of infection.

Removing Infections 4

Overview

Although far from harmless, *most* viruses that infect your machine will not destroy data, play pranks, or render your computer unusable. Even the comparatively rare viruses that do carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you actually see evidence of a payload that has activated, you will have time to deal with the infection properly. The very presence of these small snippets of unwanted computer code can, however, interfere with your computer's normal operation, consume system resources and have other undesirable effects, so you should take them seriously and be sure to remove them when you encounter them.

A second idea to keep in mind is that odd computer behavior, unexplained system crashes, or other unpredictable events might have causes other than virus infections. If you believe you have a virus on your computer because of occurrences such as these, scanning for viruses might not produce the results you expect, but it will help eliminate one potential cause of your computer problems.

The safest course of action you can take is to install VirusScan software, then scan your system immediately and thoroughly.

When you install VirusScan software, Setup starts the VirusScan application to examine your computer's memory and your hard disk boot sectors in order to verify that it can safely copy its files to your hard disk without risking their infection. If the application does not detect any infections, continue with the installation, then scan your system thoroughly as soon as you restart your computer. File-infector viruses that don't load into your computer's memory or hide in your hard disk boot blocks might still be lurking somewhere on your system.

Removing Infections Detected Upon Installation

> **TIP:** You may use the steps below when an infection has been detected and you wish to perform a thorough cleaning of your computer.

If the VirusScan application detects a virus during Setup, you'll need to remove it from your system before you install the program. To learn how to do so, refer to the steps below.

IMPORTANT: To ensure maximum security, you should also follow these same steps if a VirusScan component detects a virus in your computer's memory at some point after installation.

If VirusScan software found an infection during installation, follow these steps carefully:

1. Quit Setup immediately, then shut down your computer.

   Be sure to turn the power to your system off completely. Do *not* press CTRL+ALT+DEL or reset your computer to restart your system—some viruses can remain intact during this type of "warm" reboot.

2. If you created a VirusScan Emergency Disk during installation, then "write-protect" the disk and insert it into your floppy drive. (See TIP.)

TIP: The VirusScan Installation CD provides you with a Bootable CD version of the emergency disk. If you did not create an emergency disk *and* your computer is configured to start with a bootable CD, then insert the VirusScan Installation CD in your CD-ROM drive before proceeding to the next step.

3. Wait at least 15 seconds, then start your computer again.

   As your computer restarts, the Emergency Disk runs a batch file that leads you through an emergency scan operation. The batch file first asks you whether you cycled the power on your computer.

4. Type ***y*** to continue, then skip to Step 7 on page 45. If you did not, type `n`, then turn your computer completely off and begin again.

   The batch file next tells you that it will start a scan operation.

5. Read the notice shown on your screen, then press any key on your keyboard to continue.

   The Emergency Disk will load the files it needs into memory. If you have extended memory on your computer, it will load its database files into that memory for faster execution.

   BOOTSCAN.EXE, the command-line scanner that comes with the Emergency Disk, will make four scanning passes to examine your hard disk boot sectors, your Master Boot Record (MBR), your system directories, program files, and other likely points of infection on all of your local computer's hard disks.

NOTE: McAfee strongly recommends that you do not interrupt the BOOTSCAN.EXE scanner as it runs its scan operation. The Emergency Disk will not detect macro viruses, script viruses, or Trojan horse programs, but it will detect common file-infecting and boot-sector viruses.

If BOOTSCAN.EXE finds a virus, it will try to clean the infected file. If it fails, it will deny access to the file and continue the scan operation. After it finishes all of its scanning passes, it shows a summary report the actions it took for each hard disk on the screen. The report tells you:

- How many files the scanner examined.
- How many files of that number are clean, or uninfected.
- How many files contain potential infections.
- How many files of that number the scanner cleaned.
- How many boot sector and MBR files the scanner examined.
- How many boot sector and MBR files contain potential infections.

If the scanner detects a virus, it beeps and reports the name and location of the virus on the screen.

6. When the scanner finishes examining your hard disk, remove the Emergency Disk from your floppy drive, then shut your computer off again.
7. When BOOTSCAN.EXE finishes examining your system, you can either:

   - **Return to working with your computer.** If BOOTSCAN.EXE did not find a virus, or if it cleaned any infected files it did find, remove the Emergency Disk from your floppy drive, then restart your computer normally. If you had planned to install VirusScan software on your computer but stopped when Setup found an infection, you can now continue with your installation.
   - **Try to clean or delete infected files yourself.** If BOOTSCAN.EXE found a virus that it could not remove, it will identify the infected files and tell you that it could not clean them, or that it does not have a current remover for the infecting virus.

   As your next step, locate and delete the infected file or files. You will need to restore any files that you delete from backup files. Be sure to check your backup files for infections also. Be sure also to use the VirusScan application at your earliest opportunity to scan your system completely in order to ensure that your system is virus-free.

Removing an Infection In Windows

When McAfee VirusScan detects a virus, an alert message displays on screen to notify you. The best course of action is to attempt to clean the infected file. Cleaning removes the virus from your personal computer or wireless device and repairs the infected file.

If **Clean** does not remove the virus from your computer or wireless device, there are other methods of virus cleansing available to you.

1. **Delete** the file. When you click delete, both the virus and the infected file are removed from your computer.

TIP: Choose delete ***only*** if a backup copy of the file is available to you.

---

2. Select **Quarantine** to isolate the infected file. Once you have quarantined the infected file, use Instant Updater to download the most current anti-virus signature files. Then you can make another attempt to clean the infected file.

   You can also attempt to obtain an antidote from A.V.E.R.T.

3. If all else fails, select **Stop** to stop scanning and use the emergency disk method of repair described in the previous section – "Removing Infections Detected Upon Installation".

Using McAfee Firewall 5

Overview

Protect yourself while online with the rock solid security of McAfee Firewall. Easy-to-use, yet highly configurable, McAfee Firewall secures your PCs connection to the Internet whether you connect via DSL, cable modem or dial-up. With its new advanced Intrusion Detection System, color coded security alerts, alert messages, detailed logging and application scan for Internet capable applications with learning mode, McAfee Firewall gives you all the power you need to control the communications into and out of your PC ensuring that your online experience will be as safe as it is enjoyable.

McAfee Firewall:

- Stops fileshare and printshare access attempts.
- Shows who is connecting (i.e.: if you allow sharing).
- Stops floods and other attack packets from being received by the Operating System.
- Blocks untrusted applications from communicating over the network.
- Detects hidden programs ("trojans") that can give remote access to your PC or reveal private information (e.g. online banking information).
- Provides detailed information about which sites you have contacted and the type of connection that was made.
- Blocks all traffic while you are away, and your PC is connected 24 hours a day.

What Comes With McAfee Firewall Software?

- **Intrusion Detection System** - Powerful, yet simple to configure, McAfee Firewall's Intrusion Detection System (IDS) detects all common attack types and other suspicious activity. Users are able to easily block all further communication from offenders.
- **System Application Scan & Learning Mode** - McAfee Firewall can be set to scan a PC for programs that can communicate over the Internet and present a list of such programs to the user. Selecting the programs you want to allow, McAfee Firewall's Learning Mode will build a custom rule for the application the first time you use it when you go online.

- **Color Coded Firewall Alerts** - Easily determine the severity of potential security threats with color coded onscreen alerts. You will quickly know the level of caution appropriate for each situation.
- **Customizable Audible Alerts** - Don't miss a security or privacy concern just because you happen not to be looking at your computer screen. You can also import their own sounds to be used as audible alerts.
- **Enhanced Graphical Display of Network Activity & Attacks** - McAfee Firewall now makes it easier than ever to determine what type of activity is taking place when you go online.
- **New OS Support** - McAfee Internet Security now supports Windows XP and Windows XP themes.

How McAfee Firewall Works

McAfee Firewall is a simple-to-operate security tool for non-technical users. It dynamically manages your computing security behind the scenes, so that you do not even have to understand networking protocols. It is custom created at the moment it is needed, and only as needed, as you go on to do something else on your computer.

McAfee Firewall filters traffic at the devices that your system uses - network cards and modems. This means that it can reject inbound traffic before that traffic can reach vital functions in your PC and before it can waste valuable system resources.

It monitors applications that are either trusted or not trusted. When trusted applications need to access a network, it manages everything in the computer to allow that application's traffic. When it detects non-trusted applications trying to access a network, it blocks all traffic to and from that application.

Some network communications are needed to maintain network-based services. These are managed through user defined rules under the SYSTEM button feature of McAfee Firewall. The default SYSTEM settings feature provides protection from hostile threats.

In addition, during the installation process, it will prompt you with some basic questions to set up McAfee Firewall to do specific tasks, according to your needs (e.g. allow sharing of files or not).

About McAfee Firewall Documentation

This Getting Started manual provides the basic information you need to install, setup and use McAfee Firewall. More detailed information on step-by-step instructions on how to perform a task within McAfee Firewall is provided via the Help files which you can access while working within the different windows and dialog boxes. You can also review the Readme.txt file which contain other general information (e.g., frequently asked questions) about the product.

McAfee Firewall On-line Help

To launch McAfee Firewall Help:

From any McAfee Firewall window, click Help.
The McAfee Firewall Help displays.

McAfee Firewall Help displays in a tri-pane format with the **Contents tab** selected. With the Contents tab selected, the left pane displays the contents of Help in a book-like format. Click a book icon–or chapter–to displays the topics in of each chapter. Use the browse tools (**<<** and **>>**) in the Help tool bar to browse the topics of each chapter

You can also search for a help topic via the Index or Find tabs.

- **Index tab**

1. In the text box, type the first few letters of the word or phrase you are looking for.
2. Locate what you are looking for; then double-click the topic or click the Display button.

- **Search tab**

  Clicking the Find tab enables you to launch a full text search. When you search for topics via the Find tab for the first time, a Find Setup Wizard is displayed. Follow the instructions on screen to setup the full text search option. After setup is complete:

1. In the text box, type the first few letters of the word or phrase you are looking for. You can also select matching words to narrow your search.
2. Once you have located what you are looking for in the display topic box, click the topic.

Frequently Asked Questions

The following are frequently asked questions that you can briefly review:

How will McAfee Firewall help me?

McAfee Firewall protects your PC at the network level. It acts as a gatekeeper, checking every data packet going in or out of your PC. It allows only what you tell it to allow.

McAfee Firewall has been designed to be easy to use, while providing you with excellent protection. Once you install and run it, it is configured to block known attacks and to ask you before allowing applications to communicate.

How is my PC at risk on the Internet?

When you connect to the Internet, you share a network with millions of people from around the world. While that is a truly wonderful and amazing accomplishment, it brings with it all the problems of being accessible to complete strangers.

When on the Internet, you need to lock down your PC. When you talk to strangers on IRC (Internet Relay Chat), be cautious of files they send you. This is one way the BO (Back Orifice) program spreads, giving people remote control of your PC. Check files you get for viruses.

When on the Internet, others can try to access your fileshares. You should check that they are not available, or else people can read and delete what is on your system.

The data you send can be seen by more people than just the intended receiver. Practically any system that is connected to any part of the network path used to relay your data packets can see what is sent. Also, it is hard to know with absolute certainty that you are talking to whom you think you are talking to.

What other protection do I need?

McAfee Firewall provides network level protection. Other important types of protection are:

- Anti-virus programs, such as ***"McAfee VirusScan"*** and ***"McAfee VirusScan Professional"***, for application-level protection.
- Logon screens and screen saver passwords to prevent unauthorized access.
- File encryption or encrypting file systems, such as ***"McAfee PGP"***, to keep information secret.
- Boot-time passwords to stop someone else from starting your PC.
- Physical access to the computer, e.g. stealing the hard drive.

A separate but also important issue is controlling access to information, misinformation and "filth" that is widely available on the Internet. You can use a number of content-filtering programs or services, such as ***"McAfee Internet Security"***, that can filter the contents of data packets or restrict access to certain sites.

Are there any data packets that McAfee Firewall cannot stop?

Inbound Data: No.

As long as McAfee Firewall supports a network device and is running, it is intercepting all incoming packets and will allow or block according to the way you have it configured. If you choose to block everything, it will.

Outbound Data: Yes and no.

McAfee Firewall intercepts outbound data packets as they are passed to the network device driver. All popular applications communicate this way. A malicious program could communicate by other means, however.

What network devices does McAfee Firewall support?

McAfee Firewall supports Ethernet and Ethernet-like devices on Microsoft Windows 95, Windows 98, Windows NT 4.0 (SP4, SP5, and SP6), Windows Me, Windows 2000 and Windows XP. This includes dial-up connections, most cable and ISDN modems and most Ethernet cards. It does not support Token Ring, FDDI, ATM, Frame Relay and other networks.

What protocols can McAfee Firewall filter?

McAfee Firewall can filter TCP/IP, UDP/IP, ICMP/IP and ARP. It intercepts all protocols, but others, such as IPX, must be either allowed or blocked - no filtering is done. The Internet uses the IP protocols. No others are sent. Also, IP networks are the most common.

How can I still be harassed, even with McAfee Firewall?

Many people use McAfee Firewall block the "nukes" that cause their IRC connections to be broken (shown in Figure 1-1). While McAfee Firewall blocks the nukes, there are other ways that attackers can still cause the connections to be broken:

- **Server-side nuking.** This is when the "nukes" are sent to the IRC server, not to your computer, telling the server that you can no longer be reached. To prevent this, the IRC server needs a firewall.

- **Flood blocking a TCP connection.** If a flood of packets is sent to you from a higher speed connection, McAfee Firewall can stop the packets, but the flood takes up all your bandwidth. Your system does not get a chance to send anything. Dial-up users are particularly vulnerable since they have the lowest speed connections.

TIP: To read about other frequently asked questions, refer to the Readme.txt file found within your software installation CD.

McAfee Firewall Configuration Assistant

Welcome Screen

The McAfee Firewall Configuration Assistant displays the first time you start McAfee Firewall. This wizard guides you through initial setup and activates McAfee Firewall on your computer. Select Back, Next, Cancel, and Finish to navigate the Configuration Assistant screens.

If you select Cancel on any Configuration Assistant screen, the activation and configuration process stops. You must complete the Configuration assistant in order to activate and use McAfee Firewall.

Please note, the Configuration Assistant cannot be started after clicking Finish. However, all preferences selected using the Configuration Assistant can be changed at any time. To change a setting, select Pick a task from the McAfee Firewall main window and follow the instructions displayed on the screen.

Network Control Settings

Network Control Settings identify how you want McAfee Firewall to respond when an application or program attempts to access the Internet; either into or out of your computer.

1. To set your Network Control settings, from the Firewall main window, select one of the following.

Internet Traffic Setting	Description
Block all	• Configures McAfee Firewall to block all Internet traffic into and out of your computer. This is the most secure Firewall setting; however, programs in your computer cannot access the Internet.
Filter	• Gives you the opportunity to decide whether an application or program in your computer will be allowed to access the Internet. If an unrecognized program attempts to access your computer from the Internet, you will also be given an opportunity to allow or block its access your computer.
Allow all	• Configures McAfee Firewall to allow all Internet traffic into and out of your computer. All applications or programs in you computer will be allowed to access the Internet; applications attempting to access your computer from the Internet will not be blocked. Allow all traffic disables all McAfee Firewall protection features and should only be used diagnostic purposes.

2. Click **Next**.

Startup Options

This screen allows you to choose how you want McAfee Firewall to respond as you start your computer.

For your convenience, recommended Startup Load Options have been pre-selected for you.

1. Select **Load McAfee Firewall automatically at startup** if you want firewall protection as you start your computer. If you do not want McAfee Firewall to start as your computer starts, then clear this check box.
2. If you want to display a McAfee Firewall icon on your Windows desktop, then select **Place a McAfee Firewall icon on the desktop**. If you do not want an icon on your Windows desktop, then clear this check box.
3. Click **Next**.

Allowed Applications Screen

During the configuration process, McAfee Firewall scanned your computer's hard disk to identify programs that use the Internet. For example, programs of this type would include Internet browsers, Internet e-mail programs, and ftp (file transfer protocol) clients. On this screen, you will identify programs that you will allow to access the Internet through your Firewall.

To allow specific programs to access the Internet, do the following:

1. From the list of applications displayed on this, check the check box corresponding with each program you will allow access to the Internet. If you do not allow any or all of the programs displayed on this screen, you will be notified when each attempts to do so and decide whether to allow access to the Internet at that time.

TIP: Other programs can be "allowed" to access the Internet upon their first attempt to connect to the Internet.

---

2. Click **Finish**.

What's next?

After you complete the steps associated with setting up your initial configuration, the following events take place:

- The Firewall service starts.
- The McAfee Firewall main window displays.
- You are now ready to start using McAfee Firewall!

Introduction to Firewall's new interface

Under the guidance of the Microsoft Corporation, McAfee introduces a new look to McAfee Firewall - the Inductive User Interface (IUI).

What is an Inductive User Interface?

An IUI is similar to common web-style design – each screen within the application focuses on a unique, clearly stated, fundamental purpose. An IUI also allows you to easily navigate from one screen to the next.

How will an IUI help me?

IUI simplifies using McAfee Firewall. On any screen within Firewall, you can easily determine how to complete a task or how to access another related or different task. You can easily navigate Firewall by selecting the **Back**, **Forward** and **Home** icons. These three icons are common to all Firewall screens.

How do I use the IUI?

First, start Firewall from the Windows Start menu.

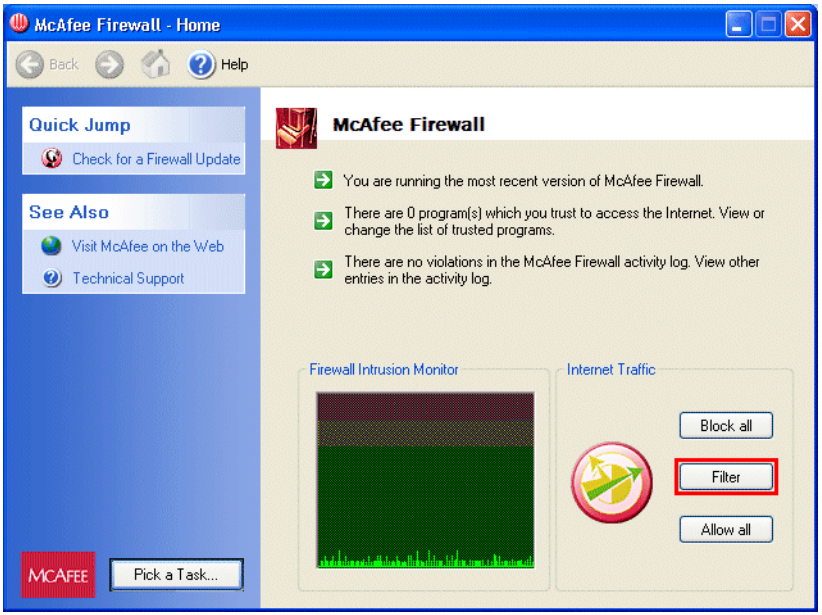


Figure 5-1. The Firewall Main Window

The Firewall main window is your central entry point to all Firewall tasks, features, and components. The main window displays three regions common to all Firewall screens.

Pick a Task

Select **Pick a task** to access the primary task screen. From the primary task screen you can select one of the following tasks:

- **Manage the programs that you trust to access to the Internet.**
- **View your computer's current Internet activity**.

- **Configure advanced settings**.
- **Set alert preferences and sounds.**
- **Shutdown Firewall and exit**.

> **TIP:** After picking a task, simply follow the on-line instructions to complete the task. If you would like to start a new task, select **Pick a task**.

Quick Jump

The **Quick Jump** section allows you access a function or program associated with McAfee Firewall (a function or program may include collection of tasks). For example, from the Quick Jump section you can:

- Click **Quick Jump** to show or hide the Quick Jump tasks.
- Select **Check for a Firewall Update** to start McAfee's Instant Updater. Instant Updater allows you to download updates to your product.

See Also

The **See Also** section displays links to external resources to help you use McAfee Firewall. From the See Also section you can:

- Click **See Also** to show or hide the See Also links.
- Select **Visit McAfee on the Web** to start your internet browser and go to www.McAfee-at-Home.com. Our McAfee-at-Home web site is a valuable resource for all of your McAfee product support needs.
- Select **Technical Support** to start your Internet browser and go to www.mcafeehelp.com. Here at www.mcafeehelp.com you will find solutions to all of your technical needs.

> **TIP:** Click **X** in the upper right corner of any Firewall screen to close the Firewall main window.

Additional status information

Depending upon your configuration, the Firewall main window displays other helpful information such as:

- Details about your version of McAfee Firewall. If there is an update to your version of McAfee Firewall available for download, pick this task.

- The number of programs that you trust to access the Internet. To view or edit the list of trusted programs, pick this task.
- Firewall violation information. Pick this task to view your Firewall violation and activity logs.

McAfee Firewall Configurations

The configuration of McAfee Firewall is divided into two parts—application (program) and system. Upon installation, a base set of rules for system services such as ICMP, DHCP and ARP are installed (these are considered default settings).

On the other hand, the programs part is personalized. Whenever you run a new program that attempts to communicate over the Internet, McAfee Firewall will prompt and ask you whether you want to trust the program or not.

For example, using Internet Explorer, enter an Internet address or URL (i.e: http://www.macafee-at-home.com) in the address bar of your browser and press ENTER. Internet Explorer will attempt to connect to that URL over the Internet. The first time you do this, McAfee Firewall prompts if you "trust" Internet Explorer. If you say "Yes", McAfee Firewall notes Internet Explorer is allowed and whenever you use Internet Explorer in the future, McAfee Firewall will allow its traffic.

Behind the scenes, McAfee Firewall creates a rule allowing Internet Explorer to communicate to the specific URL you have indicated and then deletes the rule once all traffic is received or once you exit Internet Explorer. Additionally, when trojans on your system try to communicate out from your PC, McAfee Firewall will also prompt you whether you trust them or not, and the decision to stop trojans is easy and instantaneous.

Program configuration

Default settings

During your first attempt to start McAfee Firewall, the Firewall Configuration assistant prompts you to identify programs that you will automatically allow to communicate via the Internet. Based upon the options you selected, the "firewall" reacts accordingly. That is, to either block, allow, or filter a program's communication using the Internet.

Although the Firewall setup and installation wizard performs a thorough analysis of your computer's programs–an analysis to determine programs that use the Internet to communicate–it may not have been able to identify ***all*** of your computer's programs that communicate using the Internet. Or, perhaps, you install a program after installing McAfee Firewall that uses the Internet to communicate. In these scenarios, a Firewall Communication Alert message displays as an unrecognized program attempts to communicate.

The communication alert message asks you to select one of the following options:

- **No, never**: Blocks the program's current and all future attempts to communicate. The active program is added to the trusted list of programs with an allowed state of "blocked."
- **No, not this time**: The active attempt to communicate is blocked. The program is not added to the trusted programs list.
- **Yes, this time only**: The active attempt to communicate is allowed. The program is not added to the trusted programs list.
- **Yes, always:** Allows the program's current and all future attempts to communicate. The active program is added to the trusted programs list with an allowed state of "allowed."

If you allow or block an application the first time you are prompted, McAfee Firewall provides you with the flexibility to change this setting and block or allow it to communicate at any time in the future.

As you exit McAfee Firewall, your settings are saved and will be the same the next time it is run.

Custom settings

McAfee Firewall monitors Internet traffic to see which applications are communicating. Depending on your settings, it will allow, block, or filter a program's attempt to communicate.

If you choose to "Allow all" programs to communicate through your firewall, then applications are automatically added to the "Trusted" list and will be allowed to communicate.

TIP: The Program Control window displays the current list of trusted programs and their current "allowed" state.

To view and configure the current list of trusted programs

1. From the McAfee Firewall main window select **Pick a task.**
2. From the primary task window, select **Manage the programs you trust to access the Internet**.
   Result: The Select a Program to Control window displays.
3. Select the program whose filtering settings you wish to configure (or click Browse to add a program to the list).
4. Select one of the following options:
   - Filter this programs's access to the Internet.
   - Allow this program to have full unfiltered access to the Internet.
   - Block this program from accessing the Internet.
   - Remove this program from the list.
5. Click OK.

Customized filtering rules

For all programs that you designate as "filter", McAfee Firewall provides you with the flexibility to create a set of custom filtering rules for the specific program. and can be created for any existing program that displays in the trusted programs list.

To create a custom filtering rule

1. From the **Select a program to control** window, select the program whose filtering rule you want to edit or customize.
2. Select the **Filter this program's access to the Internet** radio button.
3. Select **Customize the program's Internet filtering rules**.
   The Customize Filtering Rules window displays.

NOTE: The Customize the program's Internet filtering rules task displays if and only if the Filter this program's access to the Internet radio button is selected. For all other tasks, this task is hidden.

The Customize Filtering Rules window displays three fields (columns) for each custom rule. They are as follows:

- **Direction**: Type of Internet traffic–inbound or outbound.

- **Protocol**: Describes the type of communication protocol.
- **Port Range**: Describes the port number used by the corresponding communication protocol.

There are three tasks you can perform on the Customize Filtering Rules window. You can:

- **Change the selected filtering rule**.
  This task does not display if there are no existing custom rules.
- **Remove the selected filtering rule**.
  This task does not display if there are no existing custom rules.
- **Add a new filtering rule**.

4. Select **Add a new filtering rule**.
   The **Edit Rule** dialog box displays.
5. Click the radio button of the desired **Direction**.
6. Select a communication protocol from the **Protocol** drop-down pick list.
7. Enter a **Starting Port** number and an **Ending** Port number in their corresponding text boxes.
8. Click **OK** to add the new rule.

TIP: For more information about communication protocols, please refer to the Glossary section of this manual.

Additional information about filtering rule customization

- **To edit or change a filtering rule**, from the Customize Filtering Rules window, select the rule you want to change and click the **Change the filtering rule** task.
  Result: The Edit Rule dialog box displays. Refer to the steps described under **"To create a custom filtering rule" on page 59** to complete the task.
- **To remove a filtering rule**, from the Customize Filtering Rules window, select the rule you want to remove and click the **Remove the selected filtering rule** task.

System configuration

The operating system performs many types of network communication without reporting directly to the user. McAfee Firewall lets the user allow or block different system functions explicitly. Settings may be different for each network device, since a PC may, for example, be on an internal network as well as having a dial-up connection to the Internet.

Use the steps below to control your System settings.

1. From the McAfee Firewall main window, select **Pick a Task**.
   The primary task window displays.
2. From the primary task window, select **Configure advanced settings**.
   The Configure Advanced Settings window displays.
3. Select **Configure network adapter settings**.
4. From the Configure Network Adapter Settings window, select the adapter you want to configure and click **View or change the properties of this adapter**.
   Result: The Properties sheet for the select network adapter displays.

You can then choose to allow or block NetBIOS over TCP, Identification, ICMP, ARP, DHCP, RIP, PPTP and other protocols (IP and non-IP).

NOTE: For more information, refer to online Help or to the Glossary in this Getting Started guide.

Please refer to Table 5-1 on page 62 for a detailed description of the default settings for system activity.

Table 5-1. Default Settings for System Activity

System Activity Type	Description
NetBIOS over TCP: **Blocked**	This will block all fileshare activity over TCP as well as UDP broadcasts. Your system will not appear in anyone's "Network Neighborhood" and theirs will not appear in yours. If your system is configured to support NetBIOS over other protocols, such as IPX or NetBEUI, then filesharing may be allowed if "non-IP protocols" are allowed (see "Other Protocols" below).
Identification: **Allowed**	This service is often required when getting email and is required by most IRC servers.
ICMP: **Blocked**	This protocol is often abused as a method of breaking people's network connections (especially on IRC).
ARP: **Allowed**	ARP is a necessary Ethernet protocol and is not known to be a threat.
DHCP: **Allowed if your system uses DHCP**	The program looks in your system Registry to see if one of your network devices uses DHCP. If so, then DHCP is allowed for all devices. If not, then it is blocked for all devices. If you have more than one network device and one uses DHCP, you should check the DHCP setting for each device and allow only for the device that uses (most often cable or ADSL modems and some internal networks, not for dial-up).
RIP: **Blocked**	Allow RIP if your administrator or ISP advises you to.
PPTP: **Blocked**	This should only be altered by the administrator.
Other Protocols: **Blocked**	If you are on an IPX network, you should allow "non-IP protocols". If you use PPTP, you should allow "other IP protocols". Ask your network administrator before making any change here.

Configuration After Adding/Removing Network Devices

The System Settings must be verified after changes are made to network devices. This is especially important if a network device is added or removed. If a device was removed, all settings may have to be re-entered, because they previous settings may now be associated with the wrong device. If a device is added, it will have to be configured for the first time.

1. From the **Configure Advanced Settings** window, select **Configure network adapter settings**.

2. For each network device:

   - Select the device in the list and click the **View or change the properties of this adapter** task.

- Confirm that the settings displayed are correct. Make changes where necessary.
- Click **OK** when you are finished.

NOTE: Note: Changes take effect for this device when you choose OK on the Properties page. Choosing Cancel on the System/Settings page does not cancel these changes. If in doubt, review the settings later to confirm.

Choose OK to close the adapter's settings dialog box.

Introduction to Intrusion Detection System – (IDS)

Firewall's Intrusion Detection System (IDS) is designed to help the same users that the Personal Firewall feature protects: small offices without a corporate firewall, corporate users working outside the corporate firewall, or home users. It defends isolated machines against many different kinds of attacks (i.e.: port scans and flood attacks).

All unprotected computers can be victimized. For example, attackers can use a TCP port scan to find out what services you are running on your machine. Once this is accomplished, they can try to connect to those services and attack your machine. If the attacker discovers that you are running a TELNET, ftp, or Web server, the attacker can try each of your computer's ports sequentially, from 1 to 65535, until an open port is found that they can connect to.

Unlike other intrusion detection tools, McAfee Firewall's powerful IDS feature is simple to configure and activate. Instead of requiring users to learn and understand a complex set of attacks to build their own defense lines against intrusions, Firewall's development team created a tool that, when activated with the click of a button, detects all common attack types as well as suspicious activity.

McAfee Firewall's IDS feature looks for specific traffic patterns used by attackers. Firewall checks each packet that your machine receives to detect suspicious or known attack traffic. For example, if McAfee Firewall sees ICMP packets, it analyzes those packets for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns. When McAfee Firewall matches packets with a known attack pattern, the software generates an event to warn you of a possible security breach.

When intrusion detection is on, all traffic is checked by the intrusion detection system. When intrusion detection is active and Firewall detects an attack, you can block further communication from the suspected machine's IP address indefinitely or for a specific time period. When an attack is detected, McAfee Firewall can alert you with a Windows system tray notification.

NOTE: Because Firewall is analyzing packets and looking for patterns of packets that identify specific types of attacks, this feature may result in a very slight impact on your machine's performance.

How to Configure the Intrusion Detection System

Use the steps below to configure McAfee Firewall's intrusion detection feature:

1. Start McAfee firewall from the Windows Start menu.
   The Firewall main window displays.

TIP: Another way to start McAfee Firewall is to right-click the McAfee Guardian icon displayed in the Windows system tray, point to McAfee Firewall and select Run Firewall.

2. On the McAfee Firewall main window, select **Pick a task**.
3. Select **Advanced Firewall settings**.
4. To activate McAfee Firewall's intrusion detection system, check the **Activate Intrusion Detection** check box. Conversely, to deactivate the Intrusion detection system, clear the check mark from the **Activate Intrusion Detection** check box.
5. To block traffic from an attacker's IP address, check **Automatically block attackers**.
6. You can control how long McAfee Firewall blocks traffic from the attacker's IP address:
   - To block traffic until you remove the host, click **until removed**.
   - To block traffic from the attacker's IP address for a specific number of minutes, click **For**, and enter the **number of minutes**.
7. To play a sound when attacked, click **Play sound when attacked** and select a sound from the menu.
8. To display a Windows system tray notification, as an attack occurs, click **Show tray notification** when attached.
9. Click **OK**.

Update Your McAfee Product 6

Instant Updater

As technologies advance, we continually provide updates to McAfee software products. To ensure the highest level of protection, you should always obtain the latest version of your McAfee product.

Updating your software is simple using McAfee's Instant Updater. It is a seamless process and requires minimal interaction on your part.

IMPORTANT: Instant Updater is also the mechanism used to register your product with McAfee. In order to obtain product updates, you must register your product with McAfee.

Why Do You Need to Update?

- New features may be released for your McAfee product.
- Product fixes are periodically available.
- New product content is updated periodically.
- Updates to anti-virus signature files are frequently available.

How Does the Updating Process Work?

Instant Updater allows you to obtain and apply updates to your McAfee products while connected to the Internet. If an update exists, you will receive a notification. At that time, you can download and apply the updates to your products.

Instant Updater Features

- **Manual Updating**: If you rarely connect to the Internet, you may prefer to use Manual Updating with your McAfee product. You can manually update while connected to the Internet. To do this, select the UPDATE function from within the individual product.

TIP: Manual Updating provides you with explicit control of the updating process.

- **Auto-Inquiry**: Auto-inquiry enabled allows you to receive notification of product updates while connected to the Internet. The default setting for Instant Update is Auto-Inquiry enabled. If you do not connect to the Internet on a regular basis, you may want to disable Auto-Inquiry and use the manual update feature.

TIP: We do not recommend Auto-Inquiry enabled if you have slow internet connection.

- **Auto-Update**: If you do not want to be bothered with notification messages regarding updates, you can enable Auto-Update. Auto-Update enabled allows you to download and apply product updates without notification messages. Updates are "silently" downloaded and applied to your McAfee product.

Configuration

For additional information regarding auto-inquiry and auto-update settings, please refer to on-line help.

Product Support A

BEFORE YOU CONTACT McAfee Software for technical support, locate yourself near the computer with the McAfee product installed and verify the information listed below:

- Version number of your McAfee software

> **TIP:** From the McAfee VirusScan main window select Help > About to find this information.

- Windows operating system version number
- Amount of memory (RAM)
- Complete description of the problem
- EXACT error message as on screen
- What steps were performed prior to receiving error message?
- Is the error persistent; can you duplicate the problem
- Model name of hard disk (internal / external)
- Extra cards, boards, or hardware

How to Contact McAfee

Customer Service

To order products or obtain product information, contact the McAfee Customer Service department at (972) 308-9960 or write to the following address:

Network Associates
13465 Midway Road
Dallas, TX 75244
U.S.A.

> **NOTE:** (972) 308-9960 is telephone call to the United States of America.

www.McAfee-at-Home.com

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to your questions about McAfee Consumer Products. We encourage you to visit us at *http://www.mcafee-at-home.com* and make this your first stop for all of your product support needs.

NOTE: For a status on an existing order, you may send an e-mail message to *salesordersupport@nai.com*.

Technical Support

For agent assisted support, please visit *http://www.mcafeehelp.com*. Our support web site offers 24-hour access to solutions to the most common support requests in our easy-to-use 3 step Answer Wizard. Additionally, you may use our advanced options, which include a Keyword Search and our Help Tree, which have been designed with the more knowledgeable user in mind. If a solution to your problem cannot be found, you may also access our 24-hour FREE Chat Now! and Email Express! options. Chat and E-mail will enable you to quickly reach our qualified support engineers, through the internet, at no cost. Phone support information can also be obtained from our self-help web site at: *http://www.mcafeehelp.com*.

Virus Definition Renewal

McAfee VirusScan includes twelve (12) months of free virus protection updates obtained using Instant Updater. Renewal subscriptions are available at a cost of **$4.95 per year**.

Eleven months after registering your McAfee product, Instant Updater will prompt you to renew your virus protection subscription. You must renew your subscription in order to update your virus protection. Your product will continue to function if you do not renew your subscription.

Index

A

About McAfee Firewall 47
Allow all 53
Allowed Applications Screen 54
ARP 62
Auto-Inquiry 66
Automatic backups 40
Auto-Update 66

B

Backup strategies 41
Block all 53
blocking communications
    Personal IDS 64
Bootable CD Scans 17
BOOTSCAN.EXE
    use of on Emergency Disk 44

C

Color Coded Firewall Alerts 48
Command Prompt 17
Command-line scanners 17
Configuration after Adding/Removing Network Devices 62
Configuration Assistant 52
configure Personal IDS 63
Customizable Audible Alerts 48

D

descriptions, of VirusScan program components 15
DHCP 62
distribution of VirusScan
    electronically and on CD-ROM disc 19
Download Scan 29

E

E-Mail Scan 28
E-Mail Scan extension 16
Emergency Disk
    creation utility 17
    use of BOOTSCAN.EXE on 44
    use of to reboot system 44
End User's License Agreement 22

F

Filter 53
Flood blocking a TCP connection 52

H

HAWK 16, 29, 30
Help 27
Hostile Activity Watch Kernel 16, 30
How is my PC at risk on the Internet? 50
How McAfee Firewall works 47

I

ICMP 62
Icons 25, 55
Inbound Data 51
Inductive User Interface 25, 54
infected files
    removing viruses from 43
Installation

Autorun does not display 21
Obtained software via download 21
Instant Updater 17, 65
Internet Filter 29
Internet site filtering 28
Internet Traffic Setting 53
Intrusion Detection System 47
IPX network 62
IUI 54

L

Learning Mode 47

M

Malicious object detection and blocking 28
Managing Quarantined Files 31
Manual Updating 65
McAfee Firewall filter 51
McAfee on the Web 27, 56
MS-DOS Prompt 17
MSI 22

N

Network Control Settings 52
New product content 65

O

OAS 16
ODS 15
On-Access Scanning 16
On-access scanning 28
On-Demand Scanning 15
online help 27
Outbound Data 51

P

Palm Anti-Virus components 34
Palm OS 34
On the Device Component 35
On the PC Component Options 36
Removing Components 37
Personal IDS
blocking traffic 64
configure 63
Pick a task 26, 55
PPTP 62
Product fixes 65
Product registration 17
protocols 51

Q

Quarantine 16
Quick Jump 27
Quick Jump (section described) 56

R

reasons to run VShield 27
rebooting, with the Emergency Disk 44
responses, default, when infected by viruses 43
restarting
with the Emergency Disk 44
RIP 62

S

Safe & Sound 16
See Also 27
See Also (section described) 56
SendVirus utility 16
Server-side nuking 51

Start and Stop VShield Scanner 29
Startup Options 53
Startup Options Screen 53
Symbian's EPOC 39
    Options on the PC Component 39
Symptoms of a virus 43
System Application Scan 47
System requirements
    Desktop 19
    notebook 19
    Wireless devices 20
System Scan 28

T

Technical Support 27, 56

U

Updates to anti-virus software 65

V

Virus definition renewal 68
Virus detected 46
    upon installation 43
Virus Information Library 27
viruses
    effects of 43
    removing from infected files 43
    symptoms 43
VirusScan
    booting with Emergency Disk 44
    description of program components 15
    distribution methods 19
    features 15
    HELP 27
    Send utility 16
VShield 28
    reasons to run 27
VShield Scanner 16

W

Windows CE and Pocket PC 37
    Options on the PC Component 38
Wireless device protection 17
Wireless scanning
    What to scan
        Palm OS 36
        Symbian EPOC 39
        Windows CE, Pocket PC 38
    When to scan
        Palm OS 36
        Symbian EPOC 39
        Windows CE, Pocket PC 38
www.McAfee-at-Home.com 27, 56

For more information on products, worldwide services, and support, contact your authorized McAfee sales representative or visit us at:

Network Associates

13465 Midway Road

Dallas, TX 75244

(972) 308-9960

www.mcafee-at-home.com

NAI-518-0010-4